AMERICAN UNIVERSITY OF ARMENIA

ՀԱՅԱՍՏԱՆԻ ԱՄԵՐԻԿՅԱՆ ՀԱՄԱԼՍԱՐԱՆ

LL.M. Program

ԻՐԱՎԱԳԻՏՈՒԹՅԱՆ ՄԱԳԻՍՏՐՈՍԻ ԾՐԱԳԻՐ

TITLE

THE LIMITS OF TRADEMARK USE IN DOMAIN NAMES

"Are the rights of trademark owners duly protected against cybersquattying practices in the Republic of Armenia."

STUDENT'S NAME

Hasmik Dadasyan

SUPERVISOR'S NAME

Sarkis Knyazyan

NUMBER OF WORDS

10577

TABLE OF CONTENTS

INTRODUCTION

Branding is a central element of modern market economies and a significant part of everyday life. Companies invest large sums of money in advertising their goods and services and building a reputation in the marketplace. In turn, these activities have an impact on consumer choice and determine commercial success. The legal protection of brands is implemented through trademarks which are specific instruments of intellectual property law. In order to fulfill their economic rationale, trademark laws establish exclusive rights over distinctive marks, with the purpose of protecting the producer's investment in reputation, as well as helping consumers in differentiating among competing products.[1] Hence, the ultimate purpose of trademark protection is to prevent consumer confusion.

In the modern era of electronic commerce and other online business ventures, establishing an effective Internet presence has become a critical issue in terms of business competition. The expansion of the Internet has created a huge consumer market where many businesses not only advertise their products and services online, but also communicate with consumers directly. One of the major factors of a successful Internet presence establishment for companies is the incorporation of their trademark within the domain name of their website. Having a website with a domain name corresponding to a trademark which is well established to identify the enterprise in the real world, facilitates the establishment of identity of the enterprise over the Internet. Consumers, who are generally unaware of a domain name of a certain company, can easily find it by typing its well-known trademark. Hence, the trademarks, which perform the function of identification of enterprises in the real world, also can perform similar function in the virtual world in the form of domain names.

Nevertheless, domain names may sometimes raise trademark challenges. The roots of the conflict between domain names and trademarks are to be found in domain names registration process. The process of registration of domain names has developed in a manner that permits the grant of domain names without prior trademark review. To put it another way, the registration is done on a first come, first served basis. Domain name registrars do not conduct trademark searches before registering a new domain name. This approach was partially driven by the fact that, given the large number of domain names being registered, effective trademark searches for

[1] WIPO, *World Intellectual Property Report 2013: Brand - Reputation and Image in the Global Marketplace,* available at: https://www.wipo.int/publications/en/details.jsp?id=384, last visited 05 April 2020

all applications would place a large administrative burden on the registrars.[2] Eventually, this approach has led to the emergence of a new phenomenon, known as "cybercquatting".

Cybersquatting is the abusive registration of a domain name in violation of trademark rights. It is the process through which a party, other than the owner of a trademark, seeks to register that mark as part of a domain name with the intention of deriving economic benefit from the use of the trademark in the domain name.[3] Cybersquatters target distinctive marks for a variety of reasons. Some register well-known brand names as Internet domain names in order to extract payment from the rightful owners of the marks, who find their trademarks "locked up" and are forced to pay for the right to engage in electronic commerce under their own brand name. Others register well-known marks as domain names and warehouse those marks with the hope of selling them to the highest bidder, whether it be the trademark owner or someone else. In addition, cybersquatters often register well-known marks to prey on consumer confusion by misusing the domain name to divert customers from the mark owner's website to the cybersquatter's own website, which derive advertising revenue based on the number of visits, or "hits," the site receives. Finally, and most importantly, cybersquatters target distinctive marks to defraud consumers, including to engage in counterfeiting activities.[4] As the Director General of the United Nation's World Intellectual Property Organization (hereinafter: WIPO) Francis Gurry indicated, domain names involving fraud and phishing or counterfeit goods pose the most obvious threats, but all forms of cybersquatting affect consumers.[5]

Thus, for whatever purposes it is done, the practice of cybersquatting harms consumers, electronic commerce and the goodwill equity of valuable trademarks, upon which consumers rely to locate the true source of genuine goods and services on the Internet.[6] All of the countries in the world are, to some extent, facing the problem of abusive registrations of domain names. Some countries have already taken steps to regulate this field at the legislative level and to provide proper and adequate protection for trademark owners' rights. Unfortunately, the Republic of Armenia (hereinafter: RA) is not among those countries. The regulations provided in the legislation of RA in this regard are far from being adequate. The practice shows that, due to the gaps and shortcomings in the legislation, the only article regulating cybersquatting cases in

---

[2] Jeffrey H. Matsuura, *Managing intellectual assets in the Digital Age* § 4 (2003)
[3] *Id.*
[4] US Senate, *Report on the Anticybersquatting Consumer Protection Act*, 106th Congress Report, August 5, 1999, available at https://www.congress.gov/congressional-report/106th-congress/senate-report/140/1, last visited 05 April, 2020
[5] WIPO, *Cybersquatting Cases Grow by 12% to Reach New Record in 2018*, available at https://www.wipo.int/pressroom/en/articles/2019/article_0003.html, last visited 05 April, 2020
[6] US Senate, *supra* at 4

Armenia is being applied incorrectly by the courts. It should be realized that by letting cybersquatting cases go unpunished, they will harm consumers, electronic commerce, and the goodwill of businesses in general.[7]

Hence, the main research question of this Master's Paper is whether or not the rights of trademark owners are duly protected against cybersquattying practices in the Republic of Armenia.

The present Master's paper is based on in-depth text-based research conducted upon the international best practices, in particular official publications of WIPO, legislation of the countries that have successfully found the way to combat cybersquatting practices, legislation of the RA, analysis of legal books, journal articles and websites. In addition, cases from the practice of WIPO Arbitration and Mediation Center are examined for clarifying the interpretation of rules of Uniform Domain Name Dispute Resolution Policy (hereinafter: UDRP), the main regulatory document concerning abusive registrations of domain names.

Master's paper literature is based on a number of research articles, legal journals, academic papers, as well as guides and reports. Some legal acts such as laws and policies are also cited in the paper, namely the UDRP, the Lanham Act and Anti-Cybersquatting Consumer Protection Act of the United States of America, Domain Name Act of Finland, Postal and Electronic Communications Code of France, Act on Cybersquatting of Belgium, and finally Law on Trademarks of the RA.

[7] Lilit Karapetyan, Note, *Resolution of Trademarks and Domain Names Disputes: Armenian Regulations and International Best Practices*, 2018

CHAPTER 1

Legal Regulation of Abusive Registrations of Domain Names under the UDRP

In the late 1990s the misuse of trademarks in the domain name system reached to such a level, where it began to undermine electronic commerce and harm consumers. Trademark owners have been battling thousands of cases of cybersquatting, the vast majority of which could not be resolved through the existing dispute resolution mechanisms. Moreover, instances of abusive registrations continued to increase each year since there was no deterrent and incentive for cybersquatters to stop their abusive practices. The need for establishing a new global dispute resolution mechanism has become apparent.

1.1 The Birth of the UDRP. Dispute Resolution Procedure and Available Remedies

Domain name database is administered by Internet Corporation for Assigned Names and Numbers (hereinafter: ICANN), which has an exclusive direct control over the registration process of generic top-level domains (hereinafter: gTLDs) such as .com, .net, .edu, etc., as a coordinator and policy maker. At the very beginning of the establishment of ICANN, one of the core tasks assigned to it, was to solve "The Trademark Dilemma" which is described as the use of trademarks as domain names without the trademark owner's consent.[8]

One of ICANN's first steps in this regard was to approach WIPO asking to prepare a report on the conflict between trademarks and domain names. Published on 30 April 1999, the WIPO Report recommended the establishment of a mandatory administrative procedure concerning abusive registrations of domain names. The procedure would allow for a neutral venue in the context of disputes that are often international in nature. It was intended to be compulsory in the sense that each domain name applicant would, in the domain name agreement, be required to submit to the procedure if a claim was initiated against it by a third party.[9] As a result, the

[8] United States Department of Commerce, *Management of Internet Names and Addresses,* available at https://www.icann.org/resources/unthemed-pages/white-paper-2012-02-25-en, last visited 21 March, 2020

[9] WIPO, *The Management of Internet Names and Addresses: Intellectual Property Issues Final Report of the WIPO Internet Domain Name Process,* 1999, available at https://www.wipo.int/amc/en/processes/process1/report/finalreport.html, last visited 21 March, 2020

Uniform Domain Name Dispute Resolution Policy was developed by WIPO and adopted by ICANN on 26 August, 1999.

The UDRP establishes the legal framework for the resolution of disputes between a domain name registrant and a third party concerning the abusive registration and use of a domain name in the gTLDs. In addition, the UDRP applies to some country code top-level domains (hereinafter: ccTLDs) as well, those that have adopted the UDRP Policy on a voluntary basis. The list thereof is available at the website of WIPO.[10]

As it was already mentioned, the policy is mandatory for gTLD holders. All ICANN-accredited registrars that are authorized to register names in the gTLDs and those ccTLDs that have adopted the Policy, have agreed to abide by and implement the Policy. Thus, any person or entity wishing to register a domain name in the gTLDs and ccTLDs in question, is required to consent to the terms and conditions of the Policy.[11]

In addition, it should be noted that the UDRP clearly states that the registrars are not and will not be a party to any dispute between trademark owner and domain name holder. Moreover, according to the UDRP, registrars do not and will not participate in the administration or conduct of any proceeding before an administrative panel. Thereby, implementing the UDRP has also lessened the frequency with which domain name registrars have been named as parties in anti-cybersquatting and trademark infringement lawsuits, which was common in the early days of the privatized internet.[12]

To supplement the UDRP, ICANN adopted Rules for Uniform Domain Name Dispute Resolution Policy (hereinafter: UDRP Rules) that set out the procedures and other requirements for each stage of the dispute resolution administrative procedure. As to the body administering the procedure, currently there are six dispute resolution service providers accredited by ICANN. The complaint may be submitted to each of them. The list thereof is as follows:

- Arab Center for Domain Name Dispute Resolution
- Asian Domain Name Dispute Resolution Centre
- The National Arbitration Forum

---

[10] WIPO, *ccTLDs for which the WIPO Center provides dispute resolution services,* available at https://www.wipo.int/amc/en/domains/cctld/ last visited 21 March, 2020

[11] WIPO, *Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP),* available at https://www.wipo.int/amc/en/domains/guide/, last visited 21 March, 2020

[12] Brian J. Winterfeldt and Griffin M. Barnett, *Trademark Rights Protection Mechanisms in the Domain Name System: Current Landscape and Efforts to Diminish Protection*, 2017, available at https://www.winterfeldt.law/publications/trademark-rights-protection-mechanisms-in-the-domain-name-system-current-landscape-and-efforts-to-diminish-protection

- The Czech Arbitration Court Arbitration Centre for Internet Disputes
- The Canadian International Internet Dispute Resolution Centre
- The World Intellectual Property Organization.[13]

Regarding the various stages in the UDRP administrative procedure, there are five basic stages:

1. The filing of a complaint with a dispute resolution service provider,
2. The filing of a response by the person or entity against whom the complaint was made;
3. The appointment by the chosen dispute resolution service provider of an administrative panel of one or three persons who will decide the dispute;
4. The issuance of the administrative panel's decision and the notification of all relevant parties; and
5. The implementation of the administrative Panel's decision by the registrar(s) concerned should there be a decision that the domain name(s) in question be cancelled or transferred.[14]

The main advantage of the UDRP administrative procedure is that it typically provides a faster and cheaper way to resolve the dispute than going to court. The administrative procedure normally should be completed within 60 days of the date the provider receives the complaint.[15]

What concerns the decisions that the administrative panel can make, there are only three types of decisions

i. Decision in favor of the person or entity that filed the complaint and ordering that the disputed domain name be transferred to that person or entity;
ii. Decision in favor of the person or entity that filed the complaint and ordering that the disputed domain name be cancelled;
iii. Decision in favor of the domain name registrant (i.e., denying the requested remedy).[16]

[13] ICANN, List of Approved Dispute Resolution Service Providers, available at https://www.icann.org/resources/pages/providers-6d-2012-02-25-en, last visited 21 March, 2020
[14] ICANN, Rules for Uniform Domain Name Dispute Resolution Policy, available at https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en, last visited 21 March, 2020
[15] WIPO, *supra* at 11
[16] WIPO, *supra* at 11

It follows from the foregoing discussion, that the only remedies the UDRP offers to trademark owners is the cancelation or transfer of the disputed domain name. The administrative panel can award neither monetary relief judgments, nor compensating lawyers' costs.

After the decision on the dispute is issued by the administrative panel, it is implemented by the registrar with which the disputed domain name is registered at the time the decision is rendered. In accordance with paragraph 4(k) of the UDRP, the registrar is required to enforce the panel's decision during ten business days after it receives notification of the decision from the dispute resolution service provider, unless the registrar receives proper information from the domain name registrant in that ten-day period that it is appealing the decision in court.

Although the policy does not provide for challenging the decision rendered by administrative panel, it is stipulated under the UDRP that the mandatory administrative proceeding requirement shall not prevent either the respondent or the complainant from submitting the dispute to a court of competent jurisdiction for independent judgement. It is possible for a party to start a lawsuit in court either before an administrative proceeding is commenced or after the decision by administrative panel is issued in case the party is not satisfied with the outcome.[17]

To conclude, the UDRP is a dispute resolution mechanism established by the organization administering domain name system, that seeks to resolve disputes regarding the abusive registrations of domain names. Despite the fact that except for cancellation or transfer of a domain name, the policy does not provide for any other remedies, normally trademark owners prefer the UDRP proceeding to litigation in courts for the following reasons: first of all, it is faster and cheaper. Secondly, the decision-makers are experts in such areas of law as international trademark law, electronic commerce, domain name issues and the Internet. Thirdly, the procedure is international in scope: it provides a single mechanism for resolving a domain name dispute regardless of where the registrar or the domain name holder or the complainant are located.[18]

1.2 The UDRP Substantive Elements

For a UDRP complaint to succeed, the complainant must establish that the following three cumulative criteria are met:

[17] WIPO, *supra* at 11
[18] WIPO, *supra* at 11

(i) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;

(ii) the registrant of the domain name has no rights or legitimate interests in respect of the domain name;

(iii) the domain name has been registered and is being used in bad faith.[19]

1. Identity or Confusing Similarity Standard under the UDRP. The first element of the UDRP is seen by panels to serve essentially as a low-threshold, standing requirement.[20] The term "trademark or service mark" as used in the UDRP encompasses both registered and unregistered (sometimes referred to as common law) marks. To establish unregistered trademark rights for the purposes of UDRP, the complainant must show that its mark has become a distinctive identifier which consumers associate with the complainant's goods or services. Relevant evidence demonstrating such acquired distinctiveness, also referred to as secondary meaning, includes a range of factors such as the duration and nature of use of the mark, the amount of sales under the mark, the nature and extent of advertising using the mark, the degree of actual public recognition, and consumer surveys.[21] It is noteworthy, that the jurisdictions where the trademark is valid is not considered relevant to panel review under the first criteria. This is because of the global nature of Internet and domain name system.

To illustrate, in Assurances Premium SARL v. Whois Privacy Shield Services / Daisuke Yamaguchi case, the complainant was a French company which was the owner of the trademark "MASCOTTE ASSURANCES" registered in France. The company filed a complaint with WIPO asking to transfer <mascotte-assurances.com> which was registered and used in Japan. The Complainant did not have a registered trademark for MASCOTTE ASSURANCES in Japan. When assessing the first element of UDRP the panel noted, that the location of the trademark, among other things, is irrelevant for the purpose of finding rights in a trademark under the first element. Such factors will be considered by panel when assessing the third element of the UDRP, i.e. registering and using the domain name in bad faith.[22] Hence, the panel held that although the complainant did not have registered trademark rights in Japan, the first element was satisfied because the complainant had trademark rights for the disputed mark in France. Both France and

---

[19] ICANN, Uniform Domain Name Dispute Resolution Policy, available at https://www.icann.org/resources/pages/policy-2012-02-25-en, last visited 21 March, 2020

[20] WIPO, *The Uniform Domain Name Dispute Resolution Policy and WIPO*, 2011, available at https://www.wipo.int/export/sites/www/amc/en/docs/wipointaudrp.pdf

[21] WIPO, *Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition, 2017*, available at https://www.wipo.int/amc/en/domains/search/overview3.0#item28, last visited 21 March, 2020

[22] *Assurances Premium SARL v. Whois Privacy Shield Services / Daisuke Yamaguchi Case No. D2016-1425* available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2016-1425, WIPO, last visited on 20 March, 2020

Japan are civil law countries which means that only after registration of a trademark a person may seek legal protection for exclusive trademark rights. This demonstrates that the jurisdictions where the trademark is registered or used, is irrelevant under the first criteria.

As to the test for identity or confusing similarity, the examination involves a reasoned but relatively straightforward comparison between the complainant's trademark and the disputed domain name. This test typically involves a side-by-side comparison of the domain name and the textual components of the relevant trademark to assess whether the mark is recognizable within the disputed domain name.[23] In some cases, such assessment may also entail a more holistic aural or phonetic comparison of the complainant's trademark and the disputed domain name to ascertain confusing similarity.[24]

While each case is judged on its own merits, in cases where a domain name incorporates the entirety of a trademark, or where at least a dominant feature of the relevant mark is recognizable in the domain name, the domain name will normally be considered confusingly similar to that mark for purposes of UDRP standing.[25]

A domain name which consists of a common, obvious, or intentional misspelling of a trademark is typically considered by panels to be confusingly similar to the relevant mark for purposes of the first element. This stems from the fact that the domain name contains sufficiently recognizable aspects of the relevant mark. Under the second and third elements, panels will normally find that employing a misspelling in this way signals an intention on the part of the respondent to confuse users seeking the complainant's website. Examples of such typos include adjacent keyboard letters, replacement of similar-appearing characters (e.g., upper vs lower-case letters or numbers used to look like letters), the use of different letters that appear similar in different font, etc.[26]

As panel assessment of identity or confusing similarity involves comparing the domain name as an alpha-numeric combination and the textual components of the relevant mark, to the extent that design or figurative or stylized elements would be incapable of representation in domain names, these elements are largely disregarded under the first element. Such design

---

[23] *JCDecaux SA v. Super Privacy Service LTD c/o Dynadot, Case No. DCO2019-0034*, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=DCO2019-0034, last visited 21 March, 2020

[24] *Trivago N.V. v. Adam Smith, Case No. D2019-1957,* WIPO, available at https://www.wipo.int/amc/en/domains/decisions/text/2019/d2019-1957.html, last visited 21 Marhc, 2020

[25] WIPO, *supra* at 21

[26] WIPO, *supra* at 21

elements may be taken into account in limited circumstances, for example when the domain name comprises a spelled-out form of the relevant design element.[27]

On this basis, trademark registrations with design elements would *prima facie* satisfy the requirement that the complainant show "rights in a mark" for further assessment as to confusing similarity.

However, where design elements comprise the dominant portion of the relevant mark such that they effectively overtake the textual elements in prominence, or where the trademark registration entirely disclaims the textual elements (for example when the scope of protection afforded to the mark is effectively limited to its stylized elements), panels may find that the complainant's trademark registration is insufficient by itself to support standing under the UDRP.[28]

2. The Absence of Rights and Legitimate Interests of the Registrant of Domain name towards the disputed domain name. While the overall burden of proof in the UDRP proceedings is on the complainant, panels have recognized that proving that a respondent lacks rights or legitimate interests in a domain name may result in the often impossible task of "proving a negative". As such, where a complainant makes out a *prima facie* case that the respondent lacks rights or legitimate interests, the burden of proof on this element shifts to the respondent. If the respondent fails to come forward with relevant evidence demonstrating rights or legitimate interests in the domain name, the complainant is deemed to have satisfied the second element.[29]

To demonstrate rights or legitimate interests in a domain name, non-exclusive respondent defenses under the UDRP paragraph 4(c) include one of the following:

> *(i) before any notice of the dispute, the respondent's use of, or demonstrable preparations to use, the domain name in connection with a bona fide offering of goods or services.*

As expressed in the UDRP decisions, this sub-element may be satisfied by proving one of the following facts: evidence of business formation-related due diligence, legal advice or correspondence, evidence of credible investment in website development or promotional materials such as advertising, proof of a genuine business plan utilizing the domain name and

---

[27] *Worldwide IP Management Limited v. Pro Spedition / Registration Private, Domains By proxy, LLC / Zen Supplements Ltd, Case No. D2017-2403*, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2017-2403, last visited 21 March, 2020

[28] WIPO, *supra* at 21

[29] WIPO, *supra* at 21

credible signs of pursuit of the business plan, and other evidence generally pointing to a lack of indicia of cybersquatting intent.[30]

(ii) *the respondent has been commonly known by the domain name, even if he has acquired no trademark rights.*

Under this sub-element, it is not necessary for the respondent to have acquired corresponding trademark rights. The respondent must however be "commonly known" by the relevant moniker apart from the domain name. Examples of such monikers are a personal name, nickname, corporate identifier, etc.

Panels have recognized that mere registration of a domain name, even one that is comprised of a confirmed dictionary word or phrase and which may be generic with respect to certain goods or services may not by itself confer rights or legitimate interests in the domain name. Normally, in order to find rights or legitimate interests in a domain name based on the generic or dictionary meaning of a word or phrase contained therein, the domain name would need to be genuinely used or at least demonstrably intended for such use in connection with the relied-upon meaning.[31] For example, a hypothetical respondent may well have a right to a domain name "apple.com" if it uses it for a genuine site for apples as a fruit, but not if the website is designed to sell smartphones, laptops or other related items.

(iii) *the respondent is making a legitimate noncommercial or fair use of the domain name.*

The UDRP jurisprudence acknowledges that the use of a domain name for fair use such as noncommercial free speech would confirm a respondent's claim to a legitimate interest. This mainly refers to the websites with criticism content with respect to a particular trademark. Where the domain name consists of the mark plus a derogatory term, e.g., "applesucks.com", panels tend to find that the respondent has a legitimate interest in the domain name of a criticism website if such use is *prima facie* noncommercial and not misleading or false. However, as regards cases when the domain name is strictly identical to a trademark, panels sometimes take controversial stances. More specifically, in most of the cases involving criticism element, panels have held that even when such a domain name is used for genuine noncommercial free speech, it creates a risk of user confusion through impersonation. Nevertheless, in certain cases some

[30] WIPO, *supra* at 21

[31] *Shabby Chic Brands, LLC v. Belle Escape, Donna Jensen, Case No. D2012-0828*, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2012-0828, last visited 20 March, 2020

panels applying US First Amendment principles have found that a domain name identical to a trademark used for a bona fide noncommercial criticism site may support a legitimate interest. That is to say, when parties mutually select US jurisdiction to apply in addition to the UDRP, panelists tend to hold the following view: irrespective of whether the domain name as such connotes criticism, the respondent has a legitimate interest in using the trademark in the domain name of criticism website providing that such use is noncommercial and fair.[32]

As to the claims of fair use by resellers or distributors, outlined in the "Oki Data test", the following cumulative requirements will be applied in the specific conditions of a UDRP case:

- the respondent must actually be offering the goods or services at issue;
- the respondent must use the site to sell only the trademarked goods or services;
- the site must accurately and prominently disclose the registrant's relationship with the trademark holder; and
- the respondent must not try to "corner the market" in domain names that reflect the trademark.[33]

Cases applying the Oki Data test usually involve a domain name comprising a trademark plus a descriptive term such as "parts", "repairs", or "location". At the same time, the risk of misrepresentation has led panels to find that a respondent lacks rights or legitimate interests in cases involving a domain name identical to the complainant's trademark.[34]

The Oki Data test does not apply where there is any prior agreement between the parties in respect of the registration or use of domain names comprising the complainant's trademark.

3. Bad Faith Registration and Use. Under the UDRP, the bad faith is broadly understood to occur where a respondent takes unfair advantage of a complainant's mark or abuses it otherwise. To facilitate the evaluation of whether bad faith is present in a particular case, and considering that the burden of proof is on the complainant, UDRP paragraph 4(b) stipulates that any one of the following non-exclusive scenarios constitutes proof of a respondent's bad faith:

> *(i) evidence that the respondent has registered or acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain*

---

[32] *Howard Jarvis Taxpayers Association v. Paul McCauley, Case No. D2004-0014*, WIPO, available at https://www.wipo.int/amc/en/domains/decisions/html/2004/d2004-0014.html, last visited 20 March, 2020

[33] *Oki Data Americas, Inc. v. ASD, Inc. Case No. D2001-0903*, WIPO, available at https://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0903.html, , last visited 20 March 2020

[34] WIPO, *supra* at 21

name to the complainant who is the owner of the trademark or to a competitor of that complainant for a profit.

Such action is well expressed in *Volkswagen AG v. Jan-Iver Levsen*. The Complainant is one of the leading automobile manufacturers. Its products have been marketed throughout the world under the trademark "VOLKSWAGEN" and "VW" for at least 60 years. The respondent offered the complainant the disputed domain name <volkswagen.limo> for sale via phone and combined this offer for sale with the proposal to further register all domain names that are relevant to complainant's brand for a service fee of 2000 euros per month. In addition, the respondent offered the disputed domain name for sale also to the public on an online auction platform for a minimum price of 25,000 euros and a "buy-it-now" prize of 80,000 euros. It is also important to note that no content was displayed on the website to which the disputed domain name resolved. Examining the case, the panel held that the domain name was confusingly similar to the trademark of the complainant and the respondent had no rights or legitimate interests in respect of the domain name. Further, considering, firstly, the fact that the respondent knew or should have known that the disputed domain name consisted of the complainant's VOLKSWAGEN trademark when he registered the disputed domain name and, secondly, the large sale prize requested by the respondent in return for transferring the disputed domain name, the panel held that the circumstances indicated in paragraph 4(b)(i) of the Policy were fulfilled. Accordingly, the panel ordered that the disputed domain name <volkswagen.limo> be cancelled. [35]

(ii) "Engaging in a pattern" of registering a domain name in order to prevent the owner of the mark from obtaining a domain name with the mark included in it.

One of the outstanding examples of such action is the case of *Salvatore Ferragamo S.p.A v. Ying Chou.* The complainant is a famous Italian company in the business of fragrances, fine shoes, handbags and related goods. The company has been using the trademark "FERRAGAMO" since 1927. The products under the trademark at issue are sold in many countries including the United States and China. The respondent, a resident of China, has registered four domain names incorporating complainant's trademark in combination with the several generic terms. The disputed domain names are: <ferragamojapanhot.com>, <ferragamojapanstore.com>, <ferragamojptokyo.com>, <ferragamoshopjphot.com>. Out of the

[35] *Volkswagen AG v. Jan-Iver Levsen, Case No. D2015-0069*, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2015-0069, last visited 20 March 2020

four disputed domain names, only one hosts an active website. The other three did not resolve to any active website at the time of filing the complaint. In the panels view, the fact of registering four domain names that incorporate a famous trademark and do not resolve to active website provides a sufficient evidence to make a determination based upon paragraph 4(b)(ii) of the Policy. Thus, the panel holds that the respondent's action represents a pattern of conduct directed against the complainant, stopping it from reflecting its trademark in the disputed domain names. Therefore, an order to transfer the disputed domain names to the complainant was issued.[36]

(iii) *Evidence that the registration of the domain name was for the primary purpose of "disrupting the business of a competitor".*

This conduct is well demonstrated in the case of *Culligan International Company v. Kqwssa LLC / Domains by Proxy, LLC.* The complainant operates a water treatment solutions business through a global network in over 90 countries. Complainant is the registered owner of numerous national trademark registrations for the term " CULLIGAN ". The mark is used in connection with water filtration and treatment goods and services since 1938. Complainant operates its business in San Antonio, Texas, through a franchisee, under the name "Culligan of San Antonio." The latter owns the domain name <culligansw.com>. In 2008 the respondent registered <culligansanantonio.com>. Upon arrival at the website at the disputed domain name, users are redirected to the site ''www.kineticosa.com'', at which Kinetico water systems, that are competitive with those offered by Complainant, are sold. Considering the case, the panel found that the disputed domain name was registered and was being used in bad faith. In the Panel's assessment, the conduct described above is a clear example of the registration of the domain name for the purpose of disrupting the business of a competitor. For the foregoing reasons, the Panel ordered that the disputed domain name <culligansanantonio.com> be transferred to the complainant.[37]

(iv) Evidence of using the domain name to attract, for commercial gain, Internet users to the site by creating a "likelihood of confusion" on the part of users as to the relationship of the site with the complainant's mark.

---

[36] *Salvatore Ferragamo S.p.A v. Ying Chou*, *Case No. D2013-2034*, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2013-2034, last visited 20 March, 2020

[37] *Culligan International Company v. Kqwssa LLC / Domains By Proxy, LLC, Case No. D2012-2409,* WIPO, available at https://www.wipo.int/amc/es/domains/search/text.jsp?case=D2012-2409, last visited 20 March, 2020

An apparent example of such action can be found in *Canon U.S.A. Inc. v. Miniatures Town.* Canon Inc., is a multinational corporation that specializes in the manufacture and distribution of imaging and optical products, including most notably cameras and related accessories. Complainant, Canon U.S.A., Inc., is authorized by its corporate parent, Canon Inc., to use the CANON trademarks at issue in this proceeding and to obtain such relief as may be directed by the Panel. Canon has used the registered trademark "CANON" for over fifty years with regard to its goods and services. The respondent, a company based in the United States, is promoting and selling to the public counterfeit "Canon" lens cups and lens mugs that bear false reproductions of the "Canon" trademarks. This is done through the websites at the following domain names: <canoncups.com>; <canonlenscup.com>; <canonlenscups.com>; <canonlensmug.com>; <canonlensmugs.com>; and <canonmugs.com>. Canon has never authorized or consented in any way to the use of its marks on any of the products offered for sale through the disputed domain names. Nor has Canon granted any license to the respondent allowing such use. In the panels view, there is sufficient evidence to indicate that the respondent has been seeking to attract Internet users to its websites by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of its websites. Hence, the panel found that the respondent acted in bad faith at the time of registration and continued to do so through the operation of the websites at the disputed domain names. Consequently, an order to transfer the disputed domain names to the complainant was issued by the panel.[38]

Given that the scenarios described in UDRP paragraph 4(b) are non-exclusive and merely illustrative, even where a complainant may not be able to demonstrate the literal application of one of the above scenarios, evidence demonstrating that a respondent seeks to take unfair advantage of, abuse, or otherwise engage in behavior detrimental to the complainant's trademark would also satisfy the complainant's burden.[39]

To sum up, the UDRP furnish trademark owners with an administrative mechanism outside of the courts for cost-effective and rapid resolution of disputes arising out of the bad-faith registration and use of domain names corresponding to their trademarks. The UDRP applies to disputes in generic Top-Level Domains, as well as a growing number of country code Top-Level Domains. The leading global provider of dispute resolutions under the UDRP is United Nation's World Intellectual Property Organization. In December 1999, WIPO received the first UDRP case. Since then, trademark owners from around the world have filed over 40,000 cases with

[38] *Canon U.S.A. Inc. v. Miniatures Town, Case No. D2011-1777,* WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2011-1777, last visited 20 March 2020
[39] WIPO, *supra* at 21

WIPO. Together these WIPO cases have assisted brand owners in recovering over 75,000 domain names. Hence, it can be inferred that the UDRP has proven to be a flexible and valuable tool for brand owners in combatting the many different and new ways in which bad actors abuse trademark rights online.[40]

CHAPTER 2

Legal Regulation of Abusive Registrations of Domain Names in the United States of America and Several Other Countries

Cybersquatting practices occur in nearly every country in the world. There are different approaches in different states regarding anti-cybersquatting regulation. Some countries have developed and enacted special legislation prohibiting abusive registrations of domain names. While some others provide legal protection to trademark owners based on traditional trademark infringement and unfair competition law. Below is presented the practice of several jurisdictions

[40] WIPO, *Tackling bad faith registration of domain names in a fast-changing landscape*, available at https://www.wipo.int/wipo_magazine/en/2019/06/article_0006.html, last visited 27 March, 2020

that successfully responded to abusive registrations of domain names violating the rights of trademark owners.

United States. The Anti-Cybersquatting Consumer Protection Act. The United States was the first country in the world to respond on a legislative level to abusive registrations of domain names in the late 1990s. Before enactment of a specifically tailored anti-cybersquatting statute, trademark owners, when faced with abusive registrations of domain names, relied on traditional trademark and unfair competition law, as well as the relatively recent Federal Trademark Dilution Act (hereinafter: FTCA). All of the mentioned acts were codified in the US Trademark Act of 1946, better known as Lanham act. In applying traditional trademark infringement tests or traditional dilution principles to the cases involving abusive domain name registration, the first issue to answer was whether incorporation of the trademark in a domain name may at all amount to trademark infringement or dilution. In fact, traditional trademark infringement law aims to protect both marks and consumers against the use of trademarks in commerce in a way that may cause consumer confusion. Whereas trademark dilution rules aim to prevent commercial use of famous marks in a manner that diminishes the distinctive quality of that marks. In analyzing the question mentioned above, courts very often came to the conclusion that the existing legal tools could not adequately address the harm caused by the cybersquatting activities for the following reasons. Firstly, in both trademark and dilution doctrines, the hallmarks of trademark protection remain in the principles of "use in commerce" requirement. Since cybersquatting may occur simply in a way of mere registration of a domain name for the purposes of selling it later to the trademark owner or just to prevent the owner of the mark from obtaining a domain name with the mark included in it, the "use in commerce" requirement was impossible to satisfy by plaintiffs. Thus, courts have sometimes rejected to provide assistance to trademark owners, leaving them without effective judicial relief. Moreover, dilution law provides protection only to famous marks, whereas trademarks, that are not considered to be famous under FTCA, are out of scope of protection.

The trademark community's call for new legislation has found receptive sentiments in Congress. Legislators were convinced that cybersquatting activities constituted a serious threat to American consumers, businesses and e-commerce in general. They were also convinced that a new mechanism was needed to curb this threat.[41]

[41] Zohar Efroni, *Names as Domains, Names as Marks: Issues Concerning the Interface between Internet Domain Names and Trademark Rights*. Intellectual Property and Information Wealth: Issues and Practices in the Digital Age, Peter K. Yu, ed., Praeger Publishers, 2007, available at: https://ssrn.com/abstract=957750, last visited 27 March, 2020

The outcome of Congress's efforts was Anti-Cybersquatting Consumer Protection Act (hereinafter: ACPA) enacted in 1999. The ACPA amended the Lanham Act by clearly prohibiting the conduct of registering, trafficking in or using a domain name that is identical or confusingly similar to a mark or dilutive of a famous mark, with bad faith intent to profit. Under the ACPA, in order to succeed the plaintiff has to prove that the following three elements are present. First, the plaintiff must show that the mark embodied within the text of the domain name is either distinctive or famous. Second, after this classification is determined, the plaintiff must show that the domain name is identical, confusingly similar, or dilutive of a protected mark. Third, the plaintiff must prove that the defendant possessed a bad faith intent to profit when registering, trafficking in or using the protected mark as a domain name.[42] Further, the law sets forth a non-exclusive list of nine circumstances that may indicate such bad faith intent, though courts are free to find bad faith also in other circumstances. So, according to ACPA, in determining whether a person has a bad faith intent to profit, a court may consider factors such as, but not limited to:

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

---

[42] Adam Silberlight, *Domain Name Disputes Under the ACPA in the New Millennium: When is Bad Faith Intent to Profit Really Bad Faith and Has Anything Changed with the ACPA's Inception?* 13 Fordham Intell. Prop. Media &Ent. L.J. 269 (2002), available at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1255&context=iplj, last visited 27 March, 2020

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties;

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c).[43]

It becomes obvious from the foregoing lengthy list of bad faith circumstances that mere registration of a domain name, that may be identical or similar to a protected trademark, is not sufficient to prove violation against trademark rights. The trademark owner must prove the bad faith intent of the registrant based on but not restricted by the exemplary list of circumstances described in the statute.

The most important innovations of the ACPA are the replacement of the likelihood of confusion test with the "identical or confusingly similar" standard and the "use in commerce" requirement with bad faith element. In addition, it is important to note that immediately after the lengthy list of bad faith circumstances, the law provides the so-called "safe harbor provision"—a "good faith" scenario that would deny bad faith. In other words, it includes situations where the court may conclude that the registrant believed and had reasonable ground to believe that the use of the domain name was a fair use or otherwise lawful.[44]

Another important advantage of the ACPA is that it clearly states that a person shall be liable for using a domain name only if that person is the domain name registrant or that registrant's authorized licensee.[45] Thus, the law eliminates the uncertainty regarding the articulation of "registering, trafficking in, or using a domain name".

It can be concluded that unlike the UDRP, the ACPA provides that an authorized licensee of a domain name registrant may also be liable for bad faith use. This stems from the fact that the UDRP is a policy that is incorporated in each gTLD registration agreement. This means, that the Policy regulates the relationship between the registrant and a third party, i.e. trademark owner.

---

[43] 15 U.S.C. § 1125 *Anti-Cybersquatting Consumer Protection Act*, available at https://www.law.cornell.edu/uscode/text/15/1125, last visited 27 March, 2020

[44] *Id.*

[45] *Id.*

Although the UDRP's articulation include not only the registration but also the use of the domain name in bad faith, it refers to the use only by the registrant.

As to the remedies that trademark owner may seek in case of satisfying all three elements of cybersquatting, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.[46] The ACPA also allows trademark holders to seek monetary damages up to 100,000 USD per infringing domain name, along with other Lanham Act remedies such as actual damages and attorneys' fees.[47] It can be inferred that the ACPA grants strong and effective remedies to trademark owners to combat cybersquatting practices.

Finland. Finland is one of the few countries in Europe that has enacted a special law on domain names which regulates legal relationships regarding all aspects of domain names including abusive registrations. The law was adopted in 2003 and is called Domain Name Act (hereinafter: DNA). The act sets out the grounds for revocation of a domain name among which are the cases of abusive registration. Under DNA, a domain name may be revoked if there are weighty reasons to suspect that the domain name is a protected trademark and trademark owner requests that the name be revoked. In addition, the law provides that the domain name holder has a right to present an acceptable reason for its right within a period of two weeks. Thus, the law stipulates that the trademark owner may claim revocation of a domain name consisting of their trademark without proving the bad faith intent of the registrant. Instead, the registrant must prove that he has reasonable rights towards domain names. Besides this provision, the law prescribes that the mere registration and "warehousing" of domain names with the aim of redelivering them later is a ground for revocation *per se*. There is also a special provision regarding typosquatting under DNA. According to it, in cases when the domain name is a derivative of a protected trademark, the trademark owner may request that the domain name be revoked, if they prove that the domain name has been registered with the obvious intent of extracting benefit or harming another.[48] Thus, in instances of typosquatting there is a higher standard of proof in comparison with cases involving direct incorporation of a trademark in a domain name.

The procedure for revocation of a domain name is administrative. Appeals against the judgment may be presented before the Administrative Court of Helsinki. As to the remedy

---

[46] *Id.*

[47] 15 U.S.C. § 1117. Recovery for violation of rights, available at https://www.law.cornell.edu/uscode/text/15/1117, last visited 27 March, 2020

[48] Domain Name Act, available at https://www.finlex.fi/en/laki/kaannokset/2003/en20030228.pdf, last visited 27 March, 2020

provided for by the Act, it is revocation of the domain name. There are no transfer or compensation of damages under the DNA.[49]

In sum, the Finnish Domain Name Act regulates the legal relationships concerning domain name registrations and provides inter alia legal means to settle the disputes between trademark owners and domain name holders. The main shortcoming of DNA, however, is the absence of bad faith intent requirement. Although it states that in case of typosquatting the trademark owner has to prove that the registration of the domain name was with the primary purpose of extracting benefit or harming another, in classic cybersquatting cases the burden of proof shifts to the registrant. Thus, in comparison with ACPA, DNA provides a little bit vague legal solution.

France. In France, regulations dealing with abusive registrations of domain names are embodied in the Postal and Electronic Communications Code (hereinafter: PECC) enacted in 2011. Article L.45-2 of the Code stipulates that the registration or renewal of a domain name can be refused or the domain name removed when it is likely to infringe intellectual property rights, unless the applicant demonstrates a legitimate interest and acts in good faith. Further, article R20-44-46 provides guidance for the analysis of legitimate interest and good faith, as well as the lack thereof. Under PECC, each of the following circumstances may characterize the existence of a legitimate interest for the holder of a domain name in terms of the application of Article L.45-2:

-to use the domain name in the context of offering goods or services, or to be able to demonstrate that it is prepared for it;

-to be known by a name that is identical or related to the domain name, even in the absence of recognized rights to this name;

-to make a non-commercial use of the domain name without intention to mislead consumers.[50]

It becomes clear from the articulation of article R20-44-46, that the list provided in the Code is non-exhaustive. There may be other circumstances for the court to consider as a legitimate interest.

As stated above, the Code also sets forth an exemplary list of "lack of good faith" circumstances. They are as follows:

i. Obtaining or requesting the registration of the domain name mainly with the purpose of selling, renting or transferring it in any way whatsoever to a public

[49] *Id.*

[50] *Postal and Electronic Communications Code*, available at https://wipolex.wipo.int/en/text/493345, last visited 27 March 2020.

body, to a local authority or to the holder of an identical or similar name and not to exploit it effectively;

ii. Obtaining or requesting the registration of a domain name mainly for the purpose of damaging the reputation of the holder of a recognized right in this name or on a similar name.

iii. Obtaining or requesting the registration of a domain name mainly for the purpose of taking advantage of the reputation of the holder of a recognized right in this name or on a similar name, by creating consumer confusion.[51]

To sum up, a general overview of the anti-cybersquatting regulations under the PECC reveals many similarities with the UDRP. The French law provides a similar test for availability of bad faith intent and legitimate rights for a domain name holder.

Belgium. The anticybersquatting solutions provided by Belgium are one of the most sophisticated in Europe. Belgium has a special act on abusive registrations called Act on Cybersquatting, enacted in 2003. In particular, the law stipulates the definition of domain name, which provides an additional clarity to disputes involving abusive domain name registrations. Further, the law prescribes that in order to prevail under the Act, claimants must prove that the following conditions are cumulatively met:

(i) the domain name is identical or confusingly similar to one of the signs or names listed in the law in respect of which they have rights or legitimate interests. Such signs include: trademarks, geographical indications, company names, etc.

(ii) the domain name registrant has no rights or legitimate interests in respect to the domain name;

(iii) the domain name has been registered with the intent to damage a third party or to take an unfair advantage over them.[52]

As to the remedies under the law, only cessation is available. However, the law stipulates that it is without prejudice to application of any relevant legislation concerning trademarks, unfair competition, geographical indications and so forth. The objective of the law is not to substitute, but to supplement the legislation. Thus, although the law does not provide for monetary damages as a remedy, the claimant may require compensation of damages on the grounds of the traditional trademark legislation. It can be concluded from the foregoing that the

[51] *Id.*

[52] Act on Cybersquatting , available at https://wipolex.wipo.int/en/text/490508, last visited 27 March, 2020

main purpose of the law is to neutralize cybersquatting practices by introducing quick adjudication on the merits, backed up by effective injunction.[53]

To conclude, different countries have different rules dealing with cybersquatting practices. The research shows that there are states that have perceived the negative consequences of abusive registrations of domain names long ago, and have accordingly taken measures to amend the legislation in order to combat such practices. The United States, France, Belgium and Finland are among those countries. Although there are some differences in the regulations provided by the mentioned states, the general approach is the same. Moreover, it may be inferred that all of them are inspired by the UDRP substantive elements test and provide rules that are one way or another reminiscent of those stipulated under the UDRP.

[53] Pantov, Ventsislav, *The Prevention of Cybersquatting in Europe: Diverging Approaches and Prospects for Harmonization* (September 10, 2013). MIPLC Master Thesis Series (2012/13). Available at SSRN: https://ssrn.com/abstract=2427582

CHAPTER 3

Legal Regulation of Trademark Use in Domain Names in the Republic of Armenia.

As opposed to the countries that have adopted special legislation preventing abusive registrations of domain names, the Republic of Armenia has not yet put much efforts in this regard. The only provision related to the relations of the trademark owner and the holder of a corresponding domain name is found in RA Law on Trademarks (hereinafter: Law) and RA Civil Code. The two legal acts stipulate the same regulation on this matter.

The Law on Trademarks regulates the relationships regarding registration, legal protection and use of trademarks and service marks. Under article 12 of the Law, the proprietor of the registered trademark shall have an exclusive right to prevent third parties to use any sign in the course of trade without his consent which:

(1) is identical to the registered trademark and is used in relation to goods and/or services for which the trademark is registered;

(2) is identical or similar to the registered trademark, which is used in relation to the goods and/or services which are identical or similar to the goods and/or services for which the trademark is registered, where the use of such sign creates a likelihood of confusion on the part of public, including association with the registered trademark;

(3) is identical or similar to the trademark registered for other goods and/or services, where the latter has a reputation in the RA and the use of that sign would cause unfair advantage for the trademark or be prejudicial to the distinctive feature or the reputation of the trademark.

Point 2(5) of the same article clarifies that one of the ways of using a trademark is using the sign on the Internet or on other global computer telecommunication networks, in particular by any modes of addressing, including Internet domains.[54]

As mentioned above, this is the only provision Armenian legislation envisages concerning abusive registrations of domain names. It becomes clear from the foregoing that there is no bad faith intent requirement in the law regarding the use of a trademark in a domain name.

[54] Law on Trademarks of the Republic of Armenia, available at https://www.aipa.am/en/TrademarkLaw/, last visited 30 March, 2020

The law merely prohibits the use of a trademark in the domain name if it is done in the course of trade. This provision entails a number of concerns.

Firstly, taking into account the fact, that abusive registrations of domain names do not always contain "in the course of trade" element, the trademark owners sometimes fall outside of the protection of the law. This refers to cases when a cybersquatter registers a domain name for the purposes of selling it later to the trademark owner or simply preventing the owner of the mark from obtaining a domain name with the mark included in it. In the aforementioned cases the perpetrator does not act in the course of trade. The mere registration of a domain name is not, in itself, a "use in the course of trade" for the purposes of trademark infringement. Hence, in such cases point 2(5) of article 12 does not protect legitimate interests of trademark owners from unlawful actions of domain name registrants.

Secondly, another requirement of the above mentioned article is the "likelihood of confusion" element. This requirement also limits the trademark owners' opportunities when facing cybersquatting practices. The problem is that in the mentioned cases there is no likelihood of confusion on the part of the public, because the cybersquatter has not resolved the domain name to any active website. Thus, consumers typing the domain name corresponding to the trademark, do not see any content that would lead to confusion as to the source of the goods or services. Hence, the likelihood of confusion requirement is another impediment for trademark owners to the implementation of their rights.

Thirdly, article 12 of the Law provides protection for trademark owners' rights only against the "use" of a trademark in domain names. This means that in cases when a cybersquatter registers a domain name but does not resolve it to any active website, the "use" of a trademark requirement is not met. Consequently, article 12 will not apply.

The negative consequences of the lack of proper legislation with regard to abusive registrations of domain names appear in the case law of RA. To illustrate, in *"Softline International" CJSC v. Samvel Zakaryan and "Dolphin" LLC*, the plaintiff has filed a claim against defendants Samvel Zakaryan and "Dolphin" LLC. "Dolphin" LLC is a registrar and has registered the disputed domain name "www.softline.am" based on the agreement for providing paid services signed with Samvel Zakaryan. In accordance with the agreement, Samvel Zakaryan became the holder of the aforementioned domain name. The plaintiff asked the court to

invalidate the agreement between Samvel Zakaryan and "Dolphin" LLC and to cancel the registration of "www.softline.am".[55]

> The court found that the claim was subject to rejection on the following grounds:
>
> Under article 14 point 5 of RA Civil Code, the protection of civil law rights shall be conducted by recognizing an avoidable transaction as invalid and applying the consequences of invalidity.
>
> A claim for recognizing an avoidable transaction to be invalid can be brought by the persons specified in RA Civil Code.
>
> Under RA Civil Code, in this case "Softline International" CJSC is not a person to brought a claim for invalidation of the contract.
>
> The registration of "www.softline.am" has not been done on the basis of a disputed contract. Therefore, the registration of the domain name cannot be recognized as invalid by the force of invalidation of the contract.[56]

Thus, the practice demonstrates that, due to the gaps in the legislation, the only article regulating trademarks and domain names cases, is being applied incorrectly by the courts.[57] As a result, trademark owners are being left without adequate and effective judicial remedies which lead them to simply ''pay off'' cybersquatters in exchange for the domain name registration.

On the other hand, the absolute prohibition of trademark use, in the course of trade, in domain names might violate legitimate interests of domain name registrants. More specifically, in instances when a person registers a domain name consisting of an identical or similar trademark of another person, but in doing so does not have an intent to extract benefit or harm that person, prohibition of trademark use seems unreasonable. That is to say, the absence of bad faith requirement in the Law may serve as a reason for depriving the registrant of a domain name of his legitimate rights. An apparent example of such situation is the case "Imex Group" LLC v. "Ideal Gas" LLC. The plaintiff brought a claim against the defendant asking the court to prevent the use of its trademark in the domain name of the defendant. The plaintiff conducts business in the field of importation, manufacture and sale of building materials and heating systems under the registered trademarks "IDEAL" and "IDEAL SYSTEMS". The defendant has registered the domain name "idealgas.am in order to promote its services in the field of testing and installation

---

[55] *Softline International" CJSC v. Samvel Zakaryan and "Dolphin" LLC*, Court Case No: EKD/2944/02/12, available at http://www.datalex.am/?app=AppCaseSearch&case_id=14355223812292813, last visited March 30, 2020

[56] *Id.*

[57] Lilit Karapetyan, *supra* at 7

of gas-cylinder equipment. After reviewing the case, the court held that the claim is justified and ordered to prohibit the defendant to use the trademark of the plaintiff in the disputed domain name.[58] Thus, disregarding the fact that the domain name incorporates the company name of the defendant and the latter did not have an intent to harm the plaintiff by registering and using the domain name, the court deprived the defendant of his legitimate rights on the domain name.

To conclude, current legislation of RA does not provide sufficient and effective legal mechanisms to resolve disputes arising out of abusive registrations of domain names violating the rights of trademark owners. Moreover, trademark owners in RA are sometimes deprived of seeking protection of their rights under the UDRP as well. This stems from the fact that ".am" and ".հայ" country code Top-Level Domains are not protected under the UDRP because "Internet Society" NGO, that manages the database of ".հայ" and ".am" Top-Level Domains based on the agreement signed with ICANN, has not adopted the Policy. Hence, trademark owners in RA are not only deprived of adequate remedies against cybersquatting practices under the domestic law, but also sometimes denied the possibility of applying to WIPO for resolving their case under the UDRP. This can be evidenced by the case "*Sabremark Limited Partnership" v. "Crossnet" LLC and Hana Soufea*. Before going to court the plaintiff filed a complaint with WIPO asking to settle the dispute arising out of the registration of "sabre.am" domain name by the defendant. The WIPO Center rejected to review the case specifying that the UDRP does not apply to ".am" ccTLD. Consequently, the plaintiff had to go to court. Although the plaintiff ultimately has won the case in the court but it required about two years for the plaintiff to get the court's ruling.[59]

All of the above considerations point to the conclusion that legislative amendments with regard to abusive registrations of domain names are a necessity for the Republic of Armenia. The international best practice, namely the regulations provided under the UDRP and the relevant laws of the US, France, Finland and Belgium, may serve as a basis for drafting a new law.

[58] *"Imex Group" LLC v. "Ideal Gas" LLC*, Court Case No: EAND/0806/02/14, available at http://www.datalex.am/?app=AppCaseSearch&case_id=1125899906876030, last visited 30 March, 2020

[59] *"Sabremark Limited Partnership" v. "Crossnet" LLC and Hana Soufea*, Court Case No EKD/4034/02/17, available at http://www.datalex.am/?app=AppCaseSearch&case_id=14355223812362013, last visited 30 March, 2020

RECOMMENDATIONS

Based on conducted research, some recommendations for improving the legal framework regarding abusive registrations of domain names in the Republic of Armenia, have been drafted. The recommendations provided below may contribute to the improvement of legal regulations in the RA and provide stronger and broader protection for trademark owners' rights against unfair actions of domain name registrants. At the same time, the recommended amendments will result in proper protection of the interests of domain name holders as well. Hence, in particular, I suggest:

- To draft a separate law which will regulate the relationships arising out of abusive registrations of domain names. The research demonstrates that countries that have enacted special legislation relating to the regulation of abusive registrations of domain names, provide a stronger protection for trademark owners' rights and at the same time protect the legitimate interests of domain name holders.
- To prohibit only abusive registrations of domain names. Clearly indicate that the bad-faith registration and/or use of a domain name that is identical or confusingly similar to a trademark of another person, is prohibited. This provision will limit the scope of application of the law only to deliberate, bad-faith, and abusive registrations of domain names in violation of the rights of trademark owners.

- To provide an exemplary list of possible circumstances that may identify the bad-faith registration and use of the trademark in domain names. This regulation will limit the court's discretion of making unjustified decisions.
- To set forth factors that will determine whether domain name holders have legitimate rights and interests in the disputed domain names. This will provide additional clarity for determining bad-faith intent of the domain name registrant and will establish legal guarantees for the protection of the rights of domain name holders.
- To define sanctions for abusive registrations of domain names, namely in the form of cancellation of the registration of the domain name; transfer of the domain name and statutory damages. Clearly indicate that statutory damages do not limit or exclude the trademark owners' rights to obtain actual damages.
- After adoption of the new law, make an amendment in the article 12, point 2(5) of the Law on Trademarks in RA, and eliminate the absolute prohibition of the trademark use, in the course of trade, in the relevant domain name.

CONCLUSION

As discussed in this Master's Paper, the phenomenon of abusive registrations of domain names, which became known as "cybersquatting", causes significant damage to trademark owners who invest a huge amount of money in building a good reputation.

Nowadays, all of the countries in the world are, to some extent, facing this kind of problem. The research shows that some countries have successfully adapted their legislation to combat cybersquatting practices. Among those countries are the US, Finland, France and Belgium. In addition, WIPO has developed the UDRP with the aim of helping to maintain the overall integrity of the Internet Domain Name System, which became an effective legal tool to prevent abusive registrations in gTLDs. Both the UDRP and the legal acts of the mentioned states clearly prohibit the deliberate, bad-faith and abusive registrations of domain names. Moreover, the mentioned legal acts provide an exemplary list of circumstances that may identify the bad faith intent of the registrant. Some of them also set forth factors that determine legitimate interests of domain name holders, which provides additional clarity for determining bad-faith intent of the domain name registrant. Another important feature that is present in all the

mentioned jurisdictions and the UDRP, is that there is no "use in commerce" requirement for trademark owners to claim violations of their rights. This is a step forward in terms of the protection of trademark rights, because as research demonstrates, the "use in commerce" requirement has constituted a serious impediment for trademark owners in efforts to protect their rights.

As opposed to the countries that have taken significant steps towards preventing abusive registrations of domain names at the legislative level, the Republic of Armenia has not yet put much efforts in this regard. The only provision Armenian legislation envisages concerning abusive registrations of domain names, entails a number of concerns. The first obstacle for trademark owners is the "use in commerce" requirement. Given that abusive registrations of domain names do not always contain "use in commerce" or as it is articulated in the Armenian legislation "in the course of trade" element, trademark owners sometimes fall outside of the protection of the law. The second is the "likelihood of confusion" element present in the article regulating the use of the trademark in domain names. This requirement also limits trademark owners' opportunities when facing cybersquatting practices. The problem is that not all the cases of cybersquatting contain "in the course of trade" and "likelihood of confusion" elements. The third impediment is that article 12 of the Law provides protection for trademark owners' rights only against the "use" of a trademark in domain names. This means that in cases when a cybersquatter registers a domain name but does not resolve it to any active website, article 12 will not apply. Hence, the conclusion based on the conducted research is that current legislation of RA does not provide sufficient and effective legal mechanisms to resolve disputes arising out of abusive registrations of domain names violating the rights of trademark owners. Moreover, trademark owners in RA are sometimes deprived of seeking protection of their rights under the UDRP as well, because ".am" and ".հայ" country code Top-Level Domains are not protected under the UDRP.

Thus, the foregoing discussion leads to the conclusion that RA needs legislative amendments with regard to abusive registrations of domain names. The practice of the US, France, Finland and Belgium, as well as the big contribution of WIPO in this regard may serve as a basis for drafting a new law. The recommendations provided in this Master's paper may also be considered by the Legislator in the course of developing new legislation.

BIBLIOGRAPHY

REGULATIONS

1. Civil Code of the Republic of Armenia, available at https://www.arlis.am/DocumentView.aspx?docid=29
2. Law on Trademarks of the Republic of Armenia, available at https://www.aipa.am/en/TrademarkLaw/
3. 15 U.S.C. § 1125 Anti-Cybersquatting Consumer Protection Act, available at https://www.law.cornell.edu/uscode/text/15/1125
4. 15 U.S.C. § 1117.Recovery for violation of rights, available at https://www.law.cornell.edu/uscode/text/15/1117
5. Domain Name Act, available at https://www.finlex.fi/en/laki/kaannokset/2003/en20030228.pdf

6. Postal and Electronic Communications Code, available at https://wipolex.wipo.int/en/text/493345
7. Act on Cybersquatting , available at https://wipolex.wipo.int/en/text/490508
8. ICANN, Rules for Uniform Domain Name Dispute Resolution Policy, available at https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en
9. ICANN, Uniform Domain Name Dispute Resolution Policy, available at https://www.icann.org/resources/pages/policy-2012-02-25-en

CASES

1. Assurances Premium SARL v. Whois Privacy Shield Services / Daisuke Yamaguchi Case No. D2016-1425, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2016-1425
2. JCDecaux SA v. Super Privacy Service LTD c/o Dynadot, Case No. DCO2019-0034, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=DCO2019-0034
3. Trivago N.V. v. Adam Smith, Case No. D2019-1957, WIPO, available at https://www.wipo.int/amc/en/domains/decisions/text/2019/d2019-1957.html
4. Worldwide IP Management Limited v. Pro Spedition / Registration Private, Domains By proxy, LLC / Zen Supplements Ltd, Case No. D2017-2403, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2017-2403
5. Shabby Chic Brands, LLC v. Belle Escape, Donna Jensen, Case No. D2012-0828, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2012-0828
6. Howard Jarvis Taxpayers Association v. Paul McCauley, Case No. D2004-0014, WIPO, available at https://www.wipo.int/amc/en/domains/decisions/html/2004/d2004-0014.html
7. Oki Data Americas, Inc. v. ASD, Inc. Case No. D2001-0903, WIPO, available at https://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0903.html
8. Volkswagen AG v. Jan-Iver Levsen, Case No. D2015-0069, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2015-0069
9. Salvatore Ferragamo S.p.A v. Ying Chou, Case No. D2013-2034, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2013-2034
10. Culligan International Company v. Kqwssa LLC / Domains By Proxy, LLC, Case No. D2012-2409, WIPO, available at https://www.wipo.int/amc/es/domains/search/text.jsp?case=D2012-2409
11. Canon U.S.A. Inc. v. Miniatures Town, Case No. D2011-1777, WIPO, available at https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2011-1777
12. Softline International" CJSC v. Samvel Zakaryan and "Dolphin" LLC, Court Case No: EKD/2944/02/12, available at http://www.datalex.am/?app=AppCaseSearch&case_id=14355223812292813
13. "Imex Group" LLC v. "Ideal Gas" LLC, Court Case No: EAND/0806/02/14, available at http://www.datalex.am/?app=AppCaseSearch&case_id=1125899906876030

14. "Sabremark Limited Partnership" v. "Crossnet" LLC and Hana Soufea, Court Case No EKD/4034/02/17, available at http://www.datalex.am/?app=AppCaseSearch&case_id=14355223812362013

OFFICIAL PUBLICATIONS

1. WIPO, *World Intellectual Property Report 2013: Brand - Reputation and Image in the Global Marketplace*, available at: https://www.wipo.int/publications/en/details.jsp?id=384
2. WIPO, *The Management of Internet Names and Addresses: Intellectual Property Issues Final Report of the WIPO Internet Domain Name Process,* 1999, available at https://www.wipo.int/amc/en/processes/process1/report/finalreport.html
3. WIPO, *Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP),* available at https://www.wipo.int/amc/en/domains/guide/
4. WIPO, *The Uniform Domain Name Dispute Resolution Policy and WIPO*, 2011, available at https://www.wipo.int/export/sites/www/amc/en/docs/wipointaudrp.pdf
5. WIPO, *Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition, 2017*, available at https://www.wipo.int/amc/en/domains/search/overview3.0#item28
6. US Senate, *Report on the Anticybersquatting Consumer Protection Act*, 106th Congress Report, August 5, 1999, available at https://www.congress.gov/congressional-report/106th-congress/senate-report/140/1, last visited 05 April, 2020
7. United States Department of Commerce, *Management of Internet Names and Addresses,* available at https://www.icann.org/resources/unthemed-pages/white-paper-2012-02-25-en

BOOKS AND JOURNAL ARTICLES

1. Jeffrey H. Matsuura, *Managing intellectual assets in the Digital Age* (2003)
2. Zohar Efroni, *Names as Domains, Names as Marks: Issues Concerning the Interface between Internet Domain Names and Trademark Rights*. Intellectual Property and Information Wealth: Issues and Practices in the Digital Age, Peter K. Yu, ed., Praeger Publishers, 2007, available at: https://ssrn.com/abstract=957750,
3. Adam Silberlight, *Domain Name Disputes Under the ACPA in the New Millennium: When is Bad Faith Intent to Profit Really Bad Faith and Has Anything Changed with the ACPA's Inception?* 13 Fordham Intell. Prop. Media &Ent. L.J. 269 (2002), available at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1255&context=iplj
4. Pantov, Ventsislav, *The Prevention of Cybersquatting in Europe: Diverging Approaches and Prospects for Harmonization* (September 10, 2013). MIPLC Master Thesis Series (2012/13). Available at SSRN: https://ssrn.com/abstract=2427582
5. Lilit Karapetyan, Resolution of Trademarks and Domain Names Disputes: Armenian Regulations and International Best Practices, 2018

WEBSITES

1. WIPO, *Cybersquatting Cases Grow by 12% to Reach New Record in 2018*, available at https://www.wipo.int/pressroom/en/articles/2019/article_0003.html
2. WIPO, *ccTLDs for which the WIPO Center provides dispute resolution services,* available at https://www.wipo.int/amc/en/domains/cctld/
3. WIPO, *Tackling bad faith registration of domain names in a fast-changing landscape*, available at https://www.wipo.int/wipo_magazine/en/2019/06/article_0006.html
4. ICANN, List of Approved Dispute Resolution Service Providers, available at https://www.icann.org/resources/pages/providers-6d-2012-02-25-en
5. Brian J. Winterfeldt and Griffin M. Barnett, *Trademark Rights Protection Mechanisms in the Domain Name System: Current Landscape and Efforts to Diminish Protection*, 2017, available at https://www.winterfeldt.law/publications/trademark-rights-protection-mechanisms-in-the-domain-name-system-current-landscape-and-efforts-to-diminish-protection